AMENDMENT AND RESPONSE UNDER 37 CFR § 1.116 – EXPEDITED PROCEDURE   **Page 7**
Serial Number: 09/518,664   Dkt: 1565.027US1
Filing Date: March 3, 2000
Title: APPARATUS AND METHOD FOR AUTOMATICALLY AUTHENTICATING A NETWORK CLIENT

REMARKS

This responds to the Office Action mailed on <u>June 15, 2005</u>.

Claims <u>1-20</u> are now pending in this application.

§103 Rejection of the Claims

Claims 1-11, 13, 15, 17-18 and 20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Khan et al. (U.S. 6,401,206) in view of Mashayekhi (U.S. 5,818,936) and further in view of Howard, Jr. et al. (U.S. 6,212,280). It is of course fundamental that in order to sustain an obviousness rejection that each and every step or element in the rejected claims must be taught or suggested in the proposed combination of references. Moreover, the proposed combination of references must not run contrary to the teachings of the individual references.

More specifically, Khan is directed to creating unique digital identities. These digital identities include biometric information, among other things. Khan, col. 3 lines 66-67 through col. 4 lines 1-4. The digital identities created are then used to create public-private key pairs. Khan, col. 7 lines 1-4. Khan does not discuss a session within the context of Applicant's claims; the only mention of a session is sessions used to interact with a user to gather personal information for purposes of initially creating that user's digital identity. Khan, col. 9 lines 19-24.

The session used in Khan lacks any teaching where it is used to further encrypt other keys as is positively recited in Applicant's independent claims. Further, the Examiner acknowledges that Khan and Mashayekhi lack any teaching of a session as defined by Applicant's claims in the present Final Office Action on page 4 second full paragraph. The purpose of the digital identity in Khan is to replace other verification techniques that a user may have to remember. Individuals may actually physically carry their digital identities with them on removable media and use it to submit it to services or other individuals for verification as to their identities. Khan, col. 13, lines 1-6.

Mashayekhi is directed to the usage of key chains. In Mashayekhi, a principal includes a key chain having a variety of keys. When a principal requests a specific resource, a novel service extracts the appropriate key from the key chain on behalf of the principal and submits it

to the specific resource for principal verification to that specific resource. Again, there is no usage of session or teaching of a session as defined by Applicant's claims in Mashayekhi and the Examiner has appeared to acknowledge this fact with the citing of the Howard reference.

Howard is directed to key management of heterogeneous cryptographic assets. In Howard, a first asset has first cryptographic information and a second cryptographic piece of information is generated in response to the first cryptographic information. The second cryptographic information is delivered at a predefined time to an asset and used to acquire the first cryptographic information for purposes of authenticating and using the asset. That is the first cryptographic piece of information is not usable until the second piece of cryptographic information is obtained. This core teaching of Howard does not teach or suggest the session that is positively recited in Applicant's independent claims.

The Examiner relies on a reference in Howard where an ATM interface is described as an example usage of a certain aspect of the Howard invention. Howard, col. 10 lines 1-11. This usage is with respect to a re-keying process. Howard defines re-keying as a process for securing a distribution of a key between two parties over a network. Howard, col. 7 lines 64-67 through col. 8 lines 5-8.

Applicant would also like to point out that the reference cited by the Examiner very clearly discusses the need and teaching of using two separate session keys during a re-keying process for the ATM interface example. Howard, col. 10 lines 5-7. That is, when a shared key is changed in Howard that shared key is distributed to the two parties using a re-keying process where two unique sessions are required. Howard fails to teach or even suggest how a single session could be used and fails to discuss sessions outside the solitary context of a re-keying process.

In contrast, Applicant's independent claims discuss a common key that is encrypted with a single or same session key. The session key is not encrypted. The example in Howard does encrypt the two sessions. Thus, Applicant respectfully disagrees that the sessions and the use of the sessions is as defined and as claimed in Applicant's independent claims.

Another point that Applicant would like to make is that the proposed combination of Khan, Mashayekhi, and Howard is not permissible for the following reasons.

AMENDMENT AND RESPONSE UNDER 37 CFR § 1.116 – EXPEDITED PROCEDURE   Page 9
Serial Number: 09/518,664   Dkt: 1565.027US1
Filing Date: March 3, 2000
Title: APPARATUS AND METHOD FOR AUTOMATICALLY AUTHENTICATING A NETWORK CLIENT

In Mashayekhi a service links keys of a keychain to requestors and resources. This service does not require interfaces on a client device. Howard admits that client or assets require its integrated key management system to properly work with one another. Thus, if Howard and Mashayekhi were combined that a key portability teaching of Mashayekhi would be forever lost. Accordingly, one of ordinary skill in the art would not have been motivated to modify Mashayekhi with the teachings of Howard. Stated another way, the teachings of Mashayekhi are lost if the integrated key management system is implemented on both sides of a transaction, since integration of legacy authentication could not be achieved with Howard absent this implementation.

Thus, the Examiner's reliance on Mashayekhi in the proposed combination runs contrary to the teachings of both Mashayekhi and Howard and this not permissible.

For these reasons, Applicant respectfully request that the rejections be withdrawn and the claims allowed.

Claims 12, 14, 16 and 19 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Khan et al. in view of Mashayekhi and further in view of Howard, Jr. et al. as applied to claims 9 and 15 above, and further in view of Spies et al. (U.S. 5,869,565). Claims 12 and 14 are dependent from independent claim 9 and claims 16 and 19 are dependent from independent claim 15; therefore for the remarks presented above with respect to claims 9 and 15, the rejections of claims 12, 14, 16, and 19 should be withdrawn and these claims allowed. Applicant respectfully requests an indication of the same.

AMENDMENT AND RESPONSE UNDER 37 CFR § 1.116 – EXPEDITED PROCEDURE
Serial Number: 09/518,664
Filing Date: March 3, 2000
Title: APPARATUS AND METHOD FOR AUTOMATICALLY AUTHENTICATING A NETWORK CLIENT

Page 10
Dkt: 1565.027US1

CONCLUSION

Applicant respectfully submits that the claims are in condition for allowance and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's attorney (513) 942-0224 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.
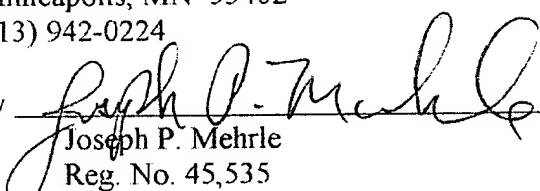
Respectfully submitted,
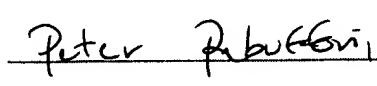
CAMERON MASHAYEKHI

By his Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
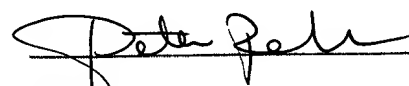P.O. Box 2938
Minneapolis, MN 55402
(513) 942-0224

Date   8-15-05   By _____
                            Joseph P. Mehrle
                            Reg. No. 45,535

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop AF, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 15 day of August, 2005.

_____   _____
Name   Signature